Homeland Security Information Bulletin
Mass Mailing Malicious Code – Worms & Viruses
June , 2003

This Bulletin is being disseminated for information purposes only. The Department of Homeland Security has noticed an increase in the use of mass mailing techniques to distribute malicious code. Several recent forms of malicious code, such as the W32/Fizzer@MM Worm (see DHS Advisory 03-#023) and the recent variations of the SOBIG virus (W32/Sobig-A, -B and –C), were propagated via e-mail.

There have been at least two variations on the mass mailing theme. In the first scenario, the virus/worm author sends e-mails with infected attachments to approximately one hundred e-mail recipients, some of whom unwittingly click on the attachment and infect their machines, which begin to send the virus/worm to all of the addresses in the recipients' e-mail address books. In this scenario the virus/worm spreads slowly, and anti-virus vendors can develop and field updated programs to their users before significant numbers of systems are impacted.

In the second scenario, the virus/worm author sends not one hundred, but thousands or millions of e-mails with infected attachments to multiple "open proxy" machines on the Internet. "Open proxies" are misconfigured computers that will accept and relay e-mail from anyone, to anyone. In this second scenario, the virus/worm author can hide the origin of the infected e-mails, because they appear to originate from the many proxy machines that forwarded them. This technique is similar to the way that spammers distribute their floods of unsolicited e-mail.

The threat that is posed by the second scenario is significant. Because the virus/worm is initially delivered simultaneously to millions of recipients, a significant portion of the recipients' machines can be infected before anti-virus vendors can update users' anti-virus programs to block the virus or worm. Those machines in turn will send infected e-mails to everyone in the infected system's address book, and the virus can spread globally in a matter of hours.

The recent Sobig mass mailer viruses (variations A, B & C) have followed a pattern in their appearance on the Internet – each new variant appeared within a day or so of when its predecessor fell dormant. The current version, Sobig-C is scheduled to expire on June 8. Security experts agree that they would not be surprised if a new variant appears this weekend (June 7-8 2003).

Organizations can protect against future e-mail delivered malicious code by blocking all executable code at their e-mail gateway. There is almost no reason why organizations should allow users to run programs arriving from the outside world, and there are many reasons why they should not. This simple countermeasure could significantly reduce the impact of mobile malicious code, including the next version of Sobig.

DHS encourages individuals to report information regarding suspicious or criminal activity to law enforcement or a Homeland Security watch office. Individuals may report incidents online at http://www.nipc.gov/incident/cirr.htm. Federal agencies/departments may report incidents online at https://incidentreport.fedcirc.gov. Contact numbers for the IAIP watch centers are: for private citizens and companies, (202) 323-3205, 1-888-585-9078 or nipc.watch@fbi.gov; for the telecom industry, (703) 607-4950 or ncs@dhs.gov; and for Federal agencies/departments, (888) 282-0870 or fedcirc@fedcirc.gov. Contact information for the FBI's field offices can be found at http://www.fbi.gov/contact/fo/fo.htm.

The links below provide additional information on the use of open proxies to distribute malicious code.

http://www.sophos.com/virusinfo/articles/sobigpattern.html/
http://www.infoworld.com/article/03/06/04/HNsobigtwo_1.html
http://www.techweb.com/wire/story/TWB20030604S0007
http://www.internetweek.com/breakingNews/showArticle.jhtml%3Bjsessionid=GXEN

DHS intends to update this Bulletin should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory Level is anticipated; the current HSAS level is YELLOW.